EXHIBIT 131

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. At a general level, my analysis of Georgia's new election equipment has revealed that, despite the addition of a paper trail, individual Georgia voters who use BMDs face security risks that are *worse* than the risks they faced when voting on DREs.

3. Paper ballots and risk-limiting audits are often thought of as the "gold standard" for election security, because, when applied in certain ways, they can detect

corresponding barcodes. Where the objective of the attack also is to alter an election outcome, the risk additionally would depend on the likelihood that attackers can compromise *sufficiently many* votes (across multiple BMDs, depending on the election) to accomplish that objective. The Plaintiffs have asked me to perform technical assessments of these risks.

6. Before the BMD-based system was introduced in Georgia, I concluded, based on the system's design and on security analyses of similar voting equipment, that the BMDs could not achieve the level of security necessary to withstand an attack by a sophisticated adversary, such as a foreign government.[1] Now, having examined in detail the equipment used in Georgia elections, as provided by Fulton County, I conclude that attackers with far fewer resources than a nation-state could carry out attacks that would alter or destroy the personal votes of individual voters and that also could alter election outcomes.

7. In September 2020, shortly before the preliminary injunction hearing, the Court authorized Plaintiffs to conduct a security examination of the voting equipment. After only a few days of investigation, I was able to demonstrate that an attacker could surreptitiously add malicious hardware to the BMD printers that would

[1] Halderman Decl. (Dec. 16, 2019), Dkt. 682 at ¶ 8.

alter the printed barcodes and change personal votes of individual voters as recorded by the election system. Although this attack would require physical access, I predicted that further investigation would establish the feasibility of attacking the BMDs directly, with software alone, in ways that could be accomplished remotely.[2]

8. These predictions have proved to be accurate. The BMDs have a series of vulnerabilities that facilitate installation of malicious software:

a) One set of vulnerabilities allows malware to be installed by anyone with brief physical access to the BMDs, potentially including voters and other members of the public.

b) Another set of vulnerabilities allows malware to spread from a county's EMS to all BMDs in the county during routine pre-election operations.

My expert report, which I will prepare and produce when it is due under a schedule entered by the Court, will describe these vulnerabilities in detail, along with several other serious vulnerabilities affecting the Georgia equipment.

9. I am also prepared to demonstrate malware that exploits these vulnerabilities, as I did with the DRE system. The malware changes barcodes on a fraction of personal ballots cast by individual voters in an election so the barcodes

[2] Tr. Dckt. 906 at 31:12-18.

encode votes for a specific candidate of the attacker's choosing when the personal vote cast by each of the affected individual voters is for a different candidate. It defeats Georgia's acceptance testing and logic and accuracy testing, as well as the additional hash verification that Pro V&V performed following the November 2020 election.[3] If this malware were used in a real election, voters and election workers would notice nothing amiss during the election since the barcodes are not human-readable, but both the scanner poll tapes and the reported totals would be fraudulent.

10. In principle, this attack could be detected by a sufficiently rigorous audit, but Georgia does not audit the human-readable ballot text at all in the vast majority of races, even high-profile ones. While the state conducted a manual audit of the November presidential contest, that audit did not examine the votes for any other contest. For example, the U.S. Senate race between Ossoff and Perdue was nearly as close as the presidential race, yet no votes in the Senate race were audited. Similarly, no audit was performed after the January Senate runoffs, despite their significance. There is no reason to believe that an attacker would necessarily target

---

[3] *See*: Secretary of State's Office, "Secretary Raffensperger announces completion of voting machine audit using forensic techniques: No sign of foul play," (Nov. 17, 2020), available at https://sos.ga.gov/index.php/elections/secretary_raffensperger_announces_completion_of_voting_machine_audit_using_forensic_techniques_no_sign_of_foul_play.

every election and every contest in Georgia, such that a sufficiently rigorous audit of one contest in one election would catch the attacker. Any given attacker could target a single contest, such as a single Senate race, especially where the outcome of a single contest can have important, far-reaching consequences, such as the circumstances of the January 2021 Senate run-off elections in Georgia, where control of the U.S. Senate by Republicans or Democrats hung in the balance.

11. Based on my experiences developing similar malware for both the DRE and BMD systems, I can compare the difficulty of attacking both types of equipment. Qualitatively, the BMD system's software stack is easier to work with, since it is based on more recent technology, yet none of the modern software defenses that have been developed since the DREs were designed was an impediment to attacking the BMDs. Quantitatively, developing the BMD malware required approximately one-third as many person-hours as developing the DRE malware. For these reasons, I conclude that outcome-changing malware is easier to create for the BMD system, and therefore Georgia's current BMD system faces an even greater risk of attack than the DRE system it replaced.

12. Beyond demonstrating the feasibility of altering personal votes cast by individual voters on individual BMDs, the Curling Plaintiffs seek to prove that such an attack could be accomplished on a wide scale, depriving them and other Georgia

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 12th day of February, 2021 in Rushland, Pennsylvania.

J. ALEX HALDERMAN